## AMENDMENTS TO THE SPECIFICATION

**In the Specification**:

Please replace page 8, lines 13-19 with the following amended paragraph:

Certificates can be utilized alone or in conjunction with other means of identification. Virtual key component [[140]] 160 is adapted to retrieve identification information from certificates. Physical key component [[150]] 170 provides a mechanism for retrieving identification information from other physical sources such as SIM cards and biometric interfaces. Identifying information provided by either or both of the virtual and physical key components can be employed to verify identity and permit access in accordance with the rules as specified in the access credential component 150.

Please replace page 11, lines 14-27 with the following amended paragraph:

Turning to Fig. 4, a certificate management system 400 is illustrated in accordance with an aspect of the present invention. Certificate management system comprises a certification component 120 and a certificate store 410. Upon generation of a certificate component 300 (Fig. 3), the component can be stored in a certificate store 410. The certificate store acts as an organized repository for certificate components. For example, certificate store 410 can store certificates as records 420 in a table of records 430. Accordingly, each record can contain ~~field~~ fields corresponding to the parts of a certificate including device ID 440 and public key 450. Once [[and]] an industrial system is properly set up in accordance with an aspect of the invention, each automation device can have a certificate stored in the certificate store which supplies, *inter alia*, an automation device name or ID and its associated public key. Thereafter, automation devices can communicate between and amongst themselves securely employing certificates, thereby allowing the identity of each device sending a message being known with a much higher degree of certainty would otherwise be known without certificates.

Please replace page 13, line 28 to page 14, line 16 with the following amended paragraph:

Turning briefly, to Fig 7, a digital signature message component 620 is illustrated in accordance with an aspect of the present invention. Digital signature message component 620 comprises a message 710. The message can be any information that an automation device would like to communicate to another automation device such as commands or a PLC program, for example. Message component also has a digital signature component 720 associated, linked, or embedded therewith. Digital signature component 720 includes message digest 722 and hash information 724. Message digest 722 contains the output value of a hash function applied to the original message 710. As discussed *supra*, the message digest is a short and fixed length representation of a longer variable length message. The message digest facilitates detection of alteration of a message in transit by comparing the provided message digest 722 with a second digest generated on the received message by the receiving entity. Hash information 724 provides data concerning the actual hash function utilized to generate the message digest (*e.g.*, MD5, SHA...). This information can then be utilized by the device receiving the digital signature message component 620 to verify that the message sent is the same message received, by generating a second message digest utilizing hash information [[722]] 724 and the received message and subsequently comparing the generated digest to the provided message digest 722. If the two digests are not the same, then the receiving entity will know that the message as been altered.